

AMENDMENT OF THE CLAIMS

Applicant offers to amend the claims as set forth below. This listing of claims reflects the claims after entry of the offered amendments, and will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method for an intermediary gateway to selectively couple an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, the method comprising:

receiving by the intermediary gateway, a secure session establishment request by the second device on the external network to establish a secure communication session with the first device on the internal network;

forwarding by the intermediary gateway, the secure session establishment request to the first device;

monitoring by the intermediary gateway, the internal network to detect an approval or disapproval acknowledgement from the first device for the secure session establishment request; and

configuring by the intermediary gateway, a first filter rule to allow communication between the first and second devices through the intermediary gateway, if an approval authentication acknowledgement is detected by the intermediary gateway;

determining by the intermediary gateway, whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, wherein the second device uses an address that is globally routable on the internal and the external networks and therefore said network traffic is valid with respect to the internal network; and

responding by the intermediary gateway, to said network traffic with an error and forcing the second device to re-establish a secure communication session from the external network.

2. (Previously Presented) The method of claim 1, further comprising:

determining by the intermediary gateway, a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

3. (Previously Presented) The method of claim 2 wherein the presence advertisement is delivered in accordance with a UPnP Simple Service Discovery Protocol (SSDP).

4. (Previously Presented) The method of claim 1, further comprising:

receiving by the intermediary gateway, network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device.

5. (Previously Presented) The method of claim 1, further comprising:

receiving by the intermediary gateway, a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determining by the intermediary gateway, the service request identifies a service advertised by the first device in a device description document; and

configuring by the intermediary gateway, a second filter rule to allow communication between the first device and the second device using the associated communication port.

6. (Previously Presented) The method of claim 1, further comprising:

providing by the intermediary gateway, the second device with an indicia for use by the second device in establishing a communication link to the first device.

7. (Cancelled)

8. (Original) The method of claim 1, wherein communication within the internal network is in accord with an IPv6 compatible Internet Protocol (IP).

9. (Previously Presented) The method of claim 1, further comprising:

retrieving by the intermediary gateway, an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and

determining by the intermediary gateway, based at least in part on the ACL, that the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

10. (Cancelled)

11. (Previously Presented) The method of claim 1, further comprising:

establishing by the intermediary gateway, the end to end secure session connection between the first device on the internal network and the second device of the external network in a single end to end secure session connection between said first and second devices.

12.-22. (Cancelled)

23. (Previously Presented) A system of devices communicatively coupled with an internal network and an external network via an intermediary gateway, comprising:

a first device, communicatively coupled to the internal network, offering services;

a second device selectively coupled with the internal and external networks and configured to use an address globally routable on the internal and the external network, the second device configured to seek a service of the first device through an intermediary gateway and to send a secure communication initiation request to the first device through an intermediary gateway to facilitate establishing a secure communication session with the first device; and

an intermediary gateway configured to selectively communicatively couple the first and second devices, wherein the intermediary gateway is configured to

receive a secure communication initiation request from the second device over the external network,

forward the request to the first device,

monitor the first device for an approval or disapproval authentication

acknowledgement for the request,

configure a filter of the intermediary gateway controlling communication over the first network from the first device based at least in part on a monitored authentication, and

determine whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, respond to said network traffic with an error and force the second device to re-establish a secure communication session from the external network.

24. (Canceled)

25. (Previously Presented) The system of claim 23, wherein the first device communicates with the second device in accord with a UPnP Security Protocol.

26. (Original) The system of claim 23, wherein the secure communication initiation request corresponds to a UPnP Set Session Key (SSK) request.

27. (Currently Amended) An article of manufacture comprising
~~a-tangible, machine-readable non-transitory accessible~~ storage medium; and
a plurality of programming instructions stored on the storage medium and configured to, when executed by an intermediary gateway, enable the intermediary gateway to selectively couple an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, including the intermediary gateway performing operations that include:

receiving a secure session establishment request by the second device on the external network to establish a secure communication session with the first device on the internal network;

forwarding the secure session establishment request to the first device;

monitoring the internal network to detect an approval or disapproval acknowledgement from the first device for the secure session establishment request; and

configuring a first filter rule to allow communication between the first and second devices through the intermediary gateway, if an approval authentication acknowledgement is detected by the intermediary gateway;

determining whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, wherein the second device uses an address that is globally routable on the internal and the external networks and therefore the network traffic is valid with respect to the internal network; and

responding to said network traffic with an error and forcing the second device to re-establish a secure communication session from the external network.

28. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the intermediate gateway to perform operations including determining that a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

29. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the intermediate gateway to perform operations including

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determining that the service request identifies a service advertised by the first device in a device description document; and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port.

30. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the intermediate gateway to perform operations including providing the second device with an indicia for use by the second device in establishing a communication link to the first device.

31. (Previously Presented) The article of manufacture of claim 27, wherein the programming instructions are further configured to enable the intermediate gateway to perform operations including

retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and

determining, based at least in part on the ACL, that the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

32.-37. (Cancelled)